一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SS2012-35 KBSE2012-37 (2012-7)

Modular GSN の定式化

猿渡 卓也[†,†2]　松野 裕[‡]　星野 隆[†2]　山本 修一郎[‡]

†名古屋大学大学院情報科学研究科 〒464-8601 愛知県名古屋市千種区不老町
‡名古屋大学情報連携統括本部 〒464-8601 愛知県名古屋市千種区不老町
†2 日本電信電話（株）ソフトウェアイノベーションセンタ 〒108-0075 東京都港区港南 2-13-34NSS2 ビル

E-mail: †2 {saruwatari_takuya_d5, hoshino.takashi}@lab.ntt.co.jp, ‡ {matsu, yamamotosui}@icts.nagoya-u.ac.jp

あらまし　システムの安全性などを保証する手段として，Assurance Case が注目されている．Assurance Case の記法として，Assurance Case の Module 化を可能とする Modular GSN が提唱されているが，明確に定義されていない．このため，本稿では，Modular GSN を形式的に定義することを試みる．

キーワード　アシュアランスケース，ディペンダビリティ，Modular GSN，GSN

Formalization of Modular GSN

Takuya SARUWATARI[†,†2] Yutaka MATSUNO[‡] Takashi HOSHINO[†2] and Shuichiro YAMAMOTO[‡]

† Graduate School of Information Science Nagoya University Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
‡ Strategy Office, Information and Communications Headquarters Nagoya University
Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
†2 NTT Software Innovation Center NSS2 building, 2-13-34 Kounan, Minatoku, Tokyo, 108-0075 Japan
E-mail: †2 {saruwatari_takuya_d5, hoshino.takashi}@lab.ntt.co.jp, ‡ {matsu, yamamotosui}@icts.nagoya-u.ac.jp

Abstract　Assurance Case attracts attention as a means to guarantee the safety of systems. Modular GSN has been proposed as the method that enabling of the Assurance Case Module. But Modular GSN has not been defined explicitly. In this paper, we define the Modular GSN formally.

Keyword　Assurance Case, Dependability, Modular GSN, GSN

1. はじめに

情報システムの用途が多様化し対象が複雑になるにつれ，情報システムの Dependability の確保が難しくなってきている．例えば，多数の機能を有するシステムでは，機能どうしが複雑に絡み合い Dependability の確保が難しくなっていると考えられる．

近年，システム開発における Dependability の確保は Assurance Case の作成という形で検討されるようになってきている[1][2]．Assurance Case の作成には，Dependability に関する要求と，その要求を保証するための議論を構造的に整理できる GSN（Goal Structuring Notation）が一般的に利用されている．GSN は Assurance Case の議論を，グラフィカルに表現することができる[3]．また，GSN の拡張として Assurance Case を複数の Module で構成する Modular GSN も提案されている[4][5]．Modular GSN の使用により，Assurance Case が複雑になり巨大化してしまった場合，Module に分割して整理することが可能となる．

Assurance Case を作成するための記法として，GSN 以外の他手法も提案されている[6][7]．これらの手法の比較や，手法同士を組み合わせた相互補完的な使用の検討が必要になってきている．この検討を実施するためには，各手法がきちんと定義されていることが望ましい．GSN については，記法を定義した例がある[8]．しかし，Modular GSN については，現状では定義が曖昧である．そこで，本稿では，Modular GSN を定式化して定義する．

本稿の構成を説明する．2 章では Assurance Case について説明する．3 章では GSN について説明する．4 章では Modular GSN について説明する．5 章では本稿において実施した Modular GSN の定式化について説明する．6 章では定式化に伴う考察を実施する．7 章では関連研究について説明する．8 章でまとめと今後の課題について述べる．

2. Assurance Case

Assurance Case とは，“システムの特性に関する重要な要求が，与えられた環境の中の適用で十分に正当化

されるという，説得力のある議論を提供する構造化された文書”[1]と定義されている．すなわち，Assurance Case とはシステムの Dependability を保証するために作成する構造的な議論のモデルであると考えることができる．近年，このような Assurance Case を使用は，徐々に広がってきている．例えば，[2]は医療用ベッドに対して Assurance Case を構築した事例である．

Assurance Case は，ゴール指向要求工学（GORE）におけるゴールグラフと類似している．しかし，GORE のゴールグラフと異なり，Assurance Case はシステム開発の上流工程のみで使用されるものではない．Assurance Case は，システム開発の企画から試験・運用・保守までにわたって作成管理される必要がある．試験・運用・保守工程から得られる試験結果等の Evidence は Assurance Case の議論を保証するために用いられる．

3. GSN

GSN（Goal Structuring Notation）とは，Assurance Case を作成するために広く利用されているグラフィカルな記法である[3]．GSN は，1）ゴール分割時の Strategy の定義が可能，2）最下層のゴールに対する Solution の付与が可能，3）Goal や Strategy に対して情報（Justification，Assumption，Model，Context）の付与が可能の 3 つの特徴を備えている．これらの特徴は，Assurance Case 作成の目的である，説得力のある議論を構造化するために必要な性質である．

GSN で作成される Assurance Case は，“Goals”，“Strategies”，“Solutions”，“Contexts”，“Assumptions”，“Justifications”の 6 つの要素と，それら要素を関係付ける“Supported by”と“In context of”の 2 つの関係からなる．Assurance Case は，これら 6 つの要素をノードとし，2 つの関係をエッジとするグラフ構造として作成される．表 1 に GSN における 6 つの要素の記法を，表 2 に 2 つの関係の記法を示す．

6 つの要素のうち，“Assumptions”，“Justifications”は，“Contexts”のサブクラスと考えることができる．本稿では，“Assumptions”，“Justifications”，“Contexts”を区別せずに“Contexts”として扱う．

表 1 要素の記法（GSN）

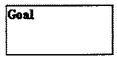
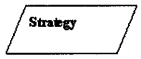
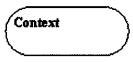
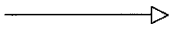
Goals	
Strategies	
Solutions	
Contexts	
Assumptions	
Justifications	

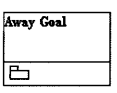
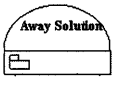
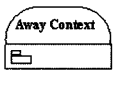
表 2 関係の記法（GSN）

Supported by	
In context of	

4. Modular GSN

Modular GSN とは，Assurance Case を Module に分割して作成するための記法であり，GSN を拡張する形で定義されている[4][5]. Modular GSN を使用することにより Assurance Case が大きくなった場合に，Module に分割して作成できる．Modular GSN では，GSN の記法に加えて Module 内から他の Module 内のノードを参照するための Away ノードの記法が定義されている[5]. 表 3 に Modular GSN で拡張された記法を示す. Modular GSN では，Assurance Case は Module 毎に表 1 表 3 の 9 つの要素をノードとし，表 2 の 2 つの関係をエッジとするグラフ構造として作成される．

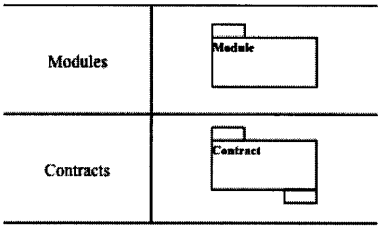
表 3 要素の記法（Modular GSN）

Away goals	
Away solutions	
Away contexts	

Modular GSN では，Module View として表 4 の“Module”と“Contract”の記法を使い Module 間の関

係を表現できる．Module Viewは，Modular GSNのグラフ全体の概要を把握するのに利用できる．

表 4 要素の記法（Module View）



5. Modular GSNの定式化

本稿では，[4][5]で提案されているModular GSNを形式的に定義し，曖昧さを排除した．以下に本稿で実施した形式的な定義を示す．尚，定義するにあたって“Assumptions”，“Justifications”，“Contexts”を区別せずに“Contexts”として扱うこととした．また，各定義における変数の具体的な値を例として示すために，図 1 の Modular GSN のグラフの各定義における値を示した．

Modular GSNグラフを，次のように定義した．

[定義]Modular GSNグラフ

Modular GSNグラフ MG=<M, Rm, Ra>は，Module集合M，Module関係集合 $Rm \subseteq M \times M$，Awayノード関係集合 $Ra \subseteq (G \times G) \cup (So \times So) \cup (C \times C)$からなる3項組みである．ここで，G，So，Cは，それぞれGoal集合，Solution集合，Context集合である．

Awayノード関係集合とは，Awayノードと実ノードとの関係を示す順序対の集合である．Awayノードとは他の実ノード（Goal，Solution，Context）を参照しているノードである．また，Away Goalは，そのモジュールの中では分解されない．

図 1 の Modular GSN グラフは，次のようになる．

M={m1, m2, m3, m4, cm1}

Rm={<m1, m2>, <m1, m3>, <m1, cm1>, <cm1, m4>}

Ra={<ag5, g5>, <ag6, g6>, <asn1, sn1>, <ac1, c1>}

Moduleを次のように定義した．

[定義]Module

Modular GSNグラフ MGのModule集合Mに含まれるModule m=<G, St, So, C, Rs, Rc>は，Goal集合G，Strategy集合St，Solution集合So，Context集合C，Supported-by 関係集合 $Rs \subseteq (G \cup St) \times (G \cup St \cup So)$，In-context-of関係集合 $Rc \subseteq (G \cup St) \times C$からなる6項組みである．

図 1 の Modular GSN のグラフでは，Module m1 は次のようになる．

G={g1, g2}

St={st1}

So={aso1}

C={ac1}

Rs={<g1, st1>, <st1, g2>, <st1, ag5>, <g2, aso1>}

Rc={<g1, ac1>}

Modular GSNのノードが定義されているModuleを返すMember-of関数を次のように定義した．

[定義]Member-of関数

関数 Member-of : $M \times (G \cup So \cup C) \rightarrow M$ は，Module mとノードx（Goal，Solution，Context）を引数にとり，xがAwayノードであれば，Awayノードの参照先である実ノードが定義されているModuleをかえし，そうでなければmを返す関数である．すなわち次の2つのケースがある．

（ケース 1）Module mのノードxが他Module m’で定義されているとき，Member-of(m,x)=m’

（ケース 2）Module mのノードxが自Module mで定義されているとき，Member-of(m,x)=m

Member-of 関数によって，モジュール内のノード（Goal，Solution，Context）は，Awayノードと，それ以外のノードとに分けられる．

図 1 の Modular GSN のグラフに対する Member-of 関数適用例を挙げると次のようになる．

Member-of(m1, g1)=m1

Member-of(m1, ac1)=m3

Member-of(m3, c1)=m3

Module間の関係とModule関係集合を次のように定義した．

[定義]Module関係

Module m，m’に対して，mにAwayノードxが存在して，Member-of(m,x)=m’となるとき，Module mとm'にはModule関係があるといい，m>m’と記述する．また，全てのModule関係の集合をModule関係集合という．Module関係集合はModule GSNグラフを構成する3項組みの1つである．

図 1 の Modular GSN のグラフでは，次の Module 関係が存在する．

m1>m2, m1>m3, m1>cm1, cm1>m4

再利用可能なModuleとしてComponent Moduleを次のように定義した．尚，Component ModuleはContract Moduleを定義するのに利用している．

[定義]Component Module

Module p,q,r が以下の条件を満たすとき，q を Component Module であるという．

（条件 1）p>q となる Module p が存在する．

（条件 2）q>r となる Module r が存在しない．

図 1 の Modular GSN グラフでは，m2，m3，m4 が Component Module となる．

Contract Module は下位の Module を再利用するための中間的な議論構造を保留するための便宜的な関係である．すなわち，Contract Module は，議論構造と再利用関係を分離するために定義される．

Module どうしの契約関係を定義する Contract Module を“Contract Module”と“Weak Contract Module”の 2 つの場合に分けて次のように定義した．尚，条件に当てはまる場合でも，Contract Module としない場合もあり得る．

[定義]Contract Module

Module m,p,q が以下の条件を満たすとき，p は Contract Module になり得る．

（条件 1）m>p となる Module m が 1 つ以上存在する．

（条件 2）p>q となる Module q が 1 つ以上存在し，q は Component Module である．

図 1 の Modular GSN グラフでは，cm1 が Contract Module になり得る．

[定義]Weak Contract Module

Module m,p,q が以下の条件を満たすとき，p は Weak Contract Module になり得る．

（条件 1）m>p となる Module m が少なくとも 1 つ存在する．

（条件 2）p>q となる Module q が少なくとも 1 つ存在する．

図 1 の Modular GSN グラフでは，cm1 が Weak Contract Module になり得る．

[定義]Modular GSN から GSN への変換

Modular GSN グラフは，GSN グラフが Module で分割されたものなので，GSN グラフに変換できる．変換後 GSN のグラフ g の各ノードの集合 G’，St’，So’，C’は，Modular GSN グラフ mg に含まれる全ての Module に含まれる全ての各ノードの集合から，Away ノードを除いた集合となる．また，各関係の集合 Rs’, Rc’は，Modular GSN グラフ mg に含まれる全てのモジュールに含まれる全ての Away ノード以外のノード間の各関係と，Away ノードを介した関係を合わせた集合となる．Away ノードを介した関係とは，ノード x, y と Away ノード z の関係において，x と z の関係が Module の Rs もしくは Rc に含まれ，かつ z と y の関係が Modular GSN グラフの Ra に含まれる時の x と y の関係である．これらの関係も Rs’あるいは Rc’に含まれる．

モジュラーGSN mg から GSN g=<G’, St’, So’, C’, Rs’, Rc’>への変換を次のように定義した．

$$G' = \{g \mid \langle G, St, So, C, Rs, Rc\rangle \in M,\ g \in G\ \wedge\ \text{Member-of}(\langle G, St, So, C, Rs, Rc\rangle, g) = \langle G, St, So, C, Rs, Rc\rangle\}$$

$$St' = \{st \mid \langle G, St, So, C, Rs, Rc\rangle \in M,\ st \in St\}$$

$$So' = \{so \mid \langle G, St, So, C, Rs, Rc\rangle \in M,\ so \in So\ \wedge\ \text{Member-of}(\langle G, St, So, C, Rs, Rc\rangle, so) = \langle G, St, So, C, Rs, Rc\rangle\}$$

$$C' = \{c \mid \langle G, St, So, C, Rs, Rc\rangle \in M,\ c \in C\ \wedge\ \text{Member-of}(\langle G, St, So, C, Rs, Rc\rangle, c) = \langle G, St, So, C, Rs, Rc\rangle\}$$

$$Rs' = \{\langle x,y\rangle \mid \langle G,St,So,C,Rs,Rc\rangle \in M, \langle x,y\rangle \in Rs\ \wedge\ \text{Member-of}(\langle G,St,So,C,Rs,Rc\rangle, y) = \langle G,St,So,C,Rs,Rc\rangle\} \cup \{\langle x,y\rangle \mid \langle G,St,So,C,Rs,Rc\rangle \in M,\ \langle x,z\rangle \in Rs\ \wedge\ \langle z,y\rangle \in Ra\ \wedge\ \neg\text{Member-of}(\langle G,St,So,C,Rs,Rc\rangle, z) = \langle G,St,So,C,Rs,Rc\rangle\}$$

$$Rc' = \{\langle x,y\rangle \mid \langle G,St,So,C,Rs,Rc\rangle \in M, \langle x,y\rangle \in Rc\ \wedge\ \text{Member-of}(\langle G,St,So,C,Rs,Rc\rangle, y) = \langle G,St,So,C,Rs,Rc\rangle\} \cup \{\langle x,y\rangle \mid \langle G,St,So,C,Rs,Rc\rangle \in M,\ \langle x,z\rangle \in Rc\ \wedge\ \langle z,y\rangle \in Ra\ \wedge\ \neg\text{Member-of}(\langle G,St,So,C,Rs,Rc\rangle, z) = \langle G,St,So,C,Rs,Rc\rangle\}$$

図 1 の Modular GSN グラフを GSN グラフに変換すると，次のように定義される．

$G'=\{g1, g2, g3, g4, g5, g6\}$

$St'=\{st1, st2\}$

$So'=\{so1, so2, so3\}$

$C'=\{c1\}$

$Rs'=\{\langle g1, st1\rangle, \langle st1, g2\rangle, \langle st1, g5\rangle, \langle g2, so1\rangle, \langle g3, so1\rangle, \langle g4, so2\rangle, \langle g5, st2\rangle, \langle st2, g6\rangle, \langle g6, so3\rangle\}$

$Rc'=\{\langle g1, c1\rangle, \langle g4, c1\rangle\}$

Modular GSN グラフの間の等価関係及び包含関係を次のように定義した．

[定義]Modular GSN の等価関係

2 つの Modular GSN グラフ M_1, M_2 が与えられた時，

M_1 と M_2 が等価であるとは，2 つの Modular GSN グラフを，それぞれ GSN グラフへ変換した G_1 と G_2 の各要素集合が全て等価であるということである．

[定義]Modular GSN の包含関係

2 つの Modular GSN グラフ M_1 と M_2 が与えられた時，$M_1 \subseteq M_2$ であるとは，2 つの Modular GSN グラフを，それぞれ GSN のグラフへ変換した G_1 と G_2 について，G_1 の各要素集合が G_2 の対応する各要素集合に全て含まれることである．

M_1 と M_2 の間に相互に包含関係が成立しているとき，即ち $M_1 \subseteq M_2$ かつ $M_2 \subseteq M_1$ の時，M_1 と M_2 は等価である．

Modular GSN のグラフ内の Module 間の結合数と Module GSN グラフの結合度を次のように定義した．

[定義]Module 間の結合数

Modular GSN グラフの 2 つの Module m1 と m2 が与えられたとき，それら Module 間の結合数を以下のように定義する．

Module 間の結合数 = |{x |Member-of(m1, x)=m2}|
+|{x |Member-of(m2, x)=m1}|

図 1 の Modular GSN のグラフにおける，m1 と m2 の間の Modular 間の結合数は 1 となる．

[定義]Module GSN グラフの結合度

Modular GSN グラフ mg が与えられたとき，mg に含まれる全ての Module の組み合わせにおける Module 間の結合数を足し合わせたものを，mg に含まれる Module の総数で割った値を mg の結合度として定義する．

図 1 の Modular GSN のグラフの結合度は，4/5 となる．

6. 考察

6.1. 定義の明確化

Modular GSN を定式化して定義する過程で，Modular GSN では以下の 3 点が明確になっていないことがわかった．そこで，本稿ではこの 3 点を以下に示すように定義した．

1. Contract Module の定義
   Contract Module の定義が曖昧であった．本稿では，以下の方針で Contract Module を定義した．
   - Contract Module は“議論構造”と“議論構造の再利用関係”を分離するために用いる特別な Module であると考える．
   - “議論構造の再利用関係”の 1 つとして Component Module を新規に定義する．
   - Component Module のみが再利用関係となり得るとする“Contract Module”と，全ての議論構造が再利用関係となり得るとする“Weak Contract Module”を定義する．
2. Away ノードとノード間の定義
   実ノードと Away ノードの関係がきちんと定義されていなかった．本稿では，実ノードへの参照である Away ノード（Away Goal, Away Solution, Away Context）と実ノード間の関係を定義した．
3. Context 付与の定義
   Context 付与の基準が不明確であった．本稿では，Context は Goal と Strategy のみに対して付与できるものと定義した．

6.2. Modular GSN のグラフの定量的評価指標

本稿では，Modular GSN のグラフに対して 1)Modular GSN の等価関係，2) Modular GSN の包含関係，3) Modular GSN のグラフの結合度を定義した．これらは，Modular GSN のグラフの比較，及び評価を実施する際に利用できる．すなわち，1) と 2) は Modular GSN により作成された 2 つのグラフについて，それら 2 つのグラフの関係を定義するのに利用できる．3) は Modular GSN のグラフを定量的に表す指標として利用できる．

7. 関連研究

ソフトウェア工学における記法を形式的に定義して理解する試みは，しばしば行われている．例えば，[9]では，要求分析結果の記法である i*Liu 法と SARM を形式化して定義し，比較している．また，Assurance Case の記法に関しても，GSN の形式的な定義が実施されている．[8]では，GSN の構成要素だけでなく，構成要素内で使う変数についての定義まで行なっている．しかし，Modular GSN に対する形式的な定義は実施されていない．本稿では，Modular GSN の定義を試みている．

ゴール指向要求工学の分野（GORE）では，ゴールグラフを利用した要求分析に関する研究が実施されてきた．代表的なゴールグラフの記法に KAOS[10], i*[11] がある．GORE では，Dependability に関連する要求についても取り扱う．しかし，GORE では基本的に要求分析のみを対象としている．本稿で，形式化を試みているのは，システム開発のライフサイクル全般における Dependability の保証を主目的とする Assurance Case の記法についてである．また，Assurance Case では Dependability に関する要求そのものだけでなく，その

要求が導出されるに至った議論を取り扱う点で GORE と異なる．

8. まとめ

本稿では，Modular GSN を定式化して定義した．その過程で，Modular GSN の曖昧だった箇所を明確にした．また，Modular GSN のグラフ同士の関係，グラフ内のモジュール結合数，及び Modular GSN グラフの結合度についても定義した．これらの新しい定義は，Modular GSN グラフの特性を理解するのに役立つと考えられる．

本稿において，Modular GSN を定義したことにより，同じように定式化された他手法との比較や補完的利用が可能になると考えている．今後は，本稿で実施した定義を利用して，他の Assurance Case の記法，ゴールグラフの記法，アーキテクチャの記法など他の技術との関係について整理していく予定である．

文　献

[1] Ankrum, T. Scott and Alfred H. Krombolz. “Structured Assurance Cases:Three Common Standards, “Slides presentation at the Association for Software Quality (ASQ) Section 509 meeting, the MITRE Corporation, 25, January 2006

[2] Mark-Alexander Sujan, Floor Koornneef, and Udo Voges, Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges, F. Saglietti and N.Oster (Eds.): SAFECOMP 2007, LNCS 4680, pp. 14-27, 2007.

[3] Kelly, Tim P. “Arguing Safety - A Systematic Approach to Safety Case Management,” DPhil Thesis, York University, Department of Computer Science Report YCST, May 1999.

[4] J. Fenn, R. Hawkins, P. Williams, and T. Kelly, “Safety case composition using contracts – refinements based on feedback from an industrial case study,” Proc. 15th Safety-Critical Sys. Symp., Feb 2007.

[5] GSN contributors, DRAFT GSN standard version 1.0, 2010.

[6] Shuichiro Yamamoto, “How Can We Cope with the Changing Requirements?,” WOSD 2011.

[7] Shuichiro Yamamoto, Yutaka Matsuno, Mario Tokoro d* framework: Inter-Dependency Model for Dependability DSN2012, 2012.

[8] Yutaka Matsuno, Kenji Taguchi, “Parameterised Argument Structure for GSN Patterns,” Quality Software (QSIC), 2011.

[9] 金子朋子，山本修一郎，田中英彦，“アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案，” Information Processing Society of Japan, 2009.

[10] Axel van Lamsweerde. “Goal-oriented requirements engineering: A guided tour,” In Proc. Of the 5th IEEE International Symposium on Requirements Engineering (RE’01), pp. 249-263, 2001.

[11] Eric S. K. Yu. “Towards Modeling and Reasoning Support for Early-Phase Requirements Engineering,” In 3rd IEEE Int. Symp on Requirements Engineering, pp. 226-235, Washington DC, Jan 1997.

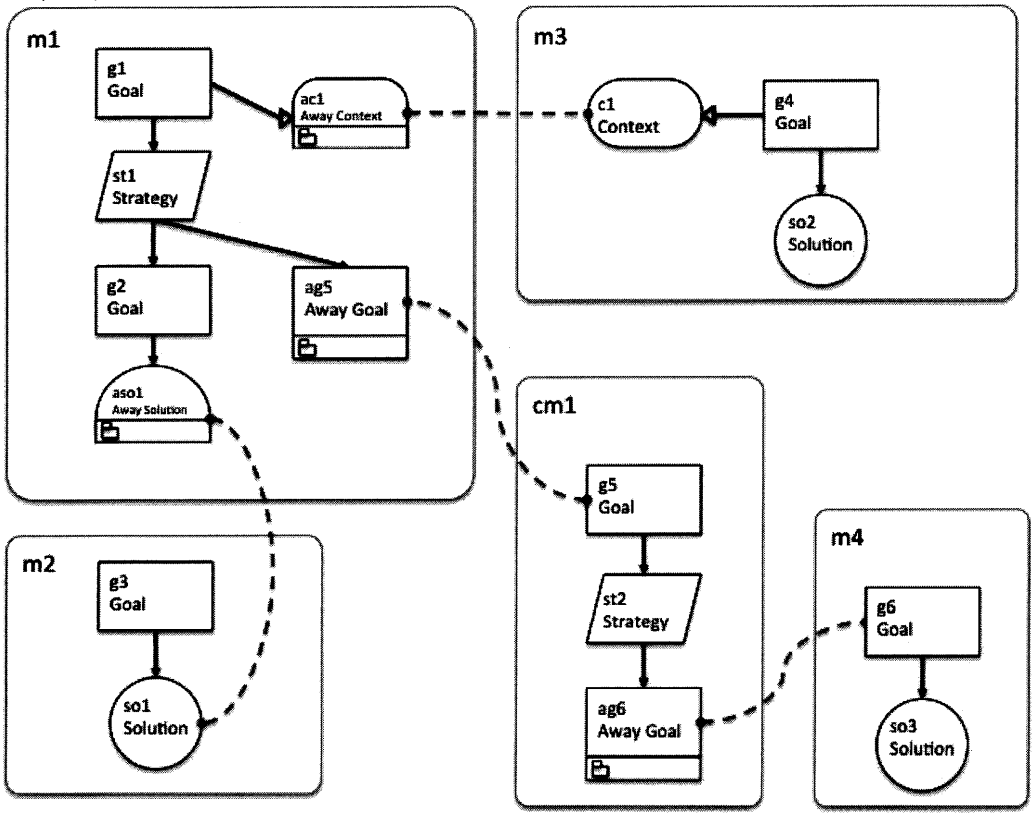


図 1 Modular GSN グラフ